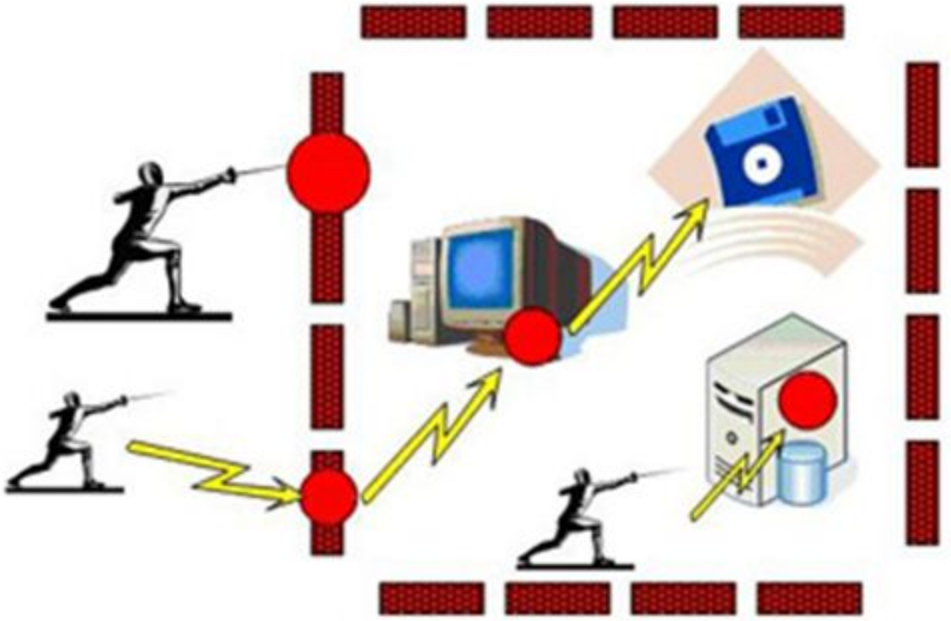
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ корпоративных информационных систем



Информационные технологии в экономике

лекция №9

1. Угрозы

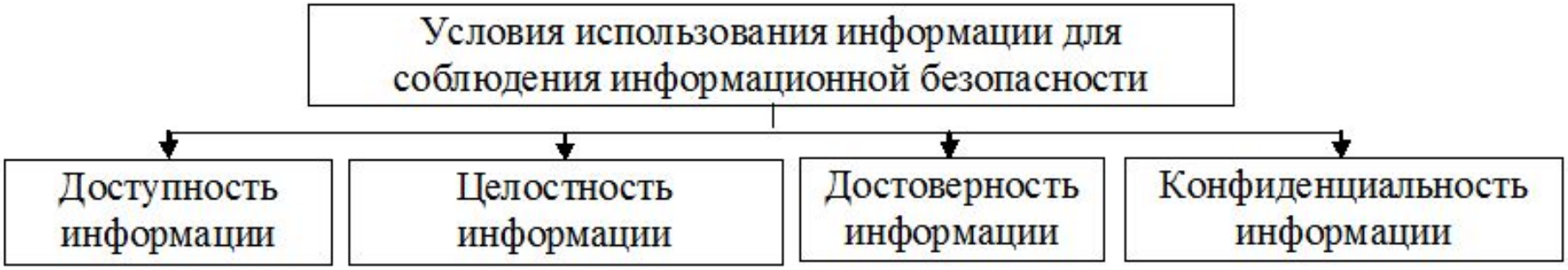


Рис. 1. Условия использования информации

Под **информационной безопасностью** понимается защищенность ресурсов ИС от факторов, представляющих угрозу для конфиденциальности, целостности и доступности информации

Виды угроз информационных систем

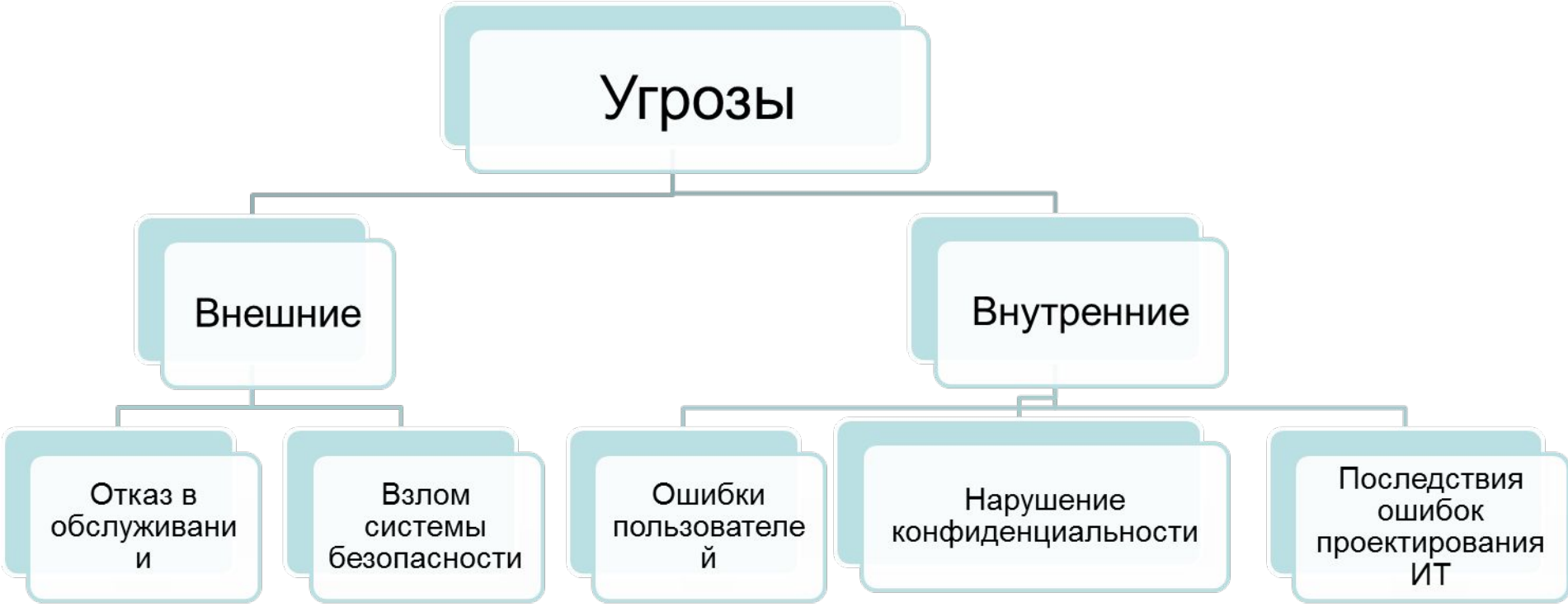


Рис. 2. Виды угроз ИС

I. Базовые принципы защищенности ИС

- 1.Наличие и полнота политики безопасности

- 2. Гарантированность безопасности

Политика безопасности

Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов

- *(organizational security policies) — совокупность руководящих принциповorganizational security policies) — совокупность руководящих принципов, правилorganizational security policies) — совокупность руководящих принципов, правил, процедурorganizational security policies) — совокупность руководящих

- *Гарантированность безопасности - мера доверия, которая может быть оказана архитектуре и реализации системы*

Стандарты безопасности:

- Стандарты и спецификации – одна из форм накопления знаний о процедурном и программно-техническом уровнях информационной безопасности и ИС.

- Стандарты и спецификации являются основными средствами обеспечения взаимной совместимости аппаратно-программных средств и их компонентов.

II.Подходы к обоснованию проекта подсистемы обеспечения безопасности

1) - проверка соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности;

$$\sum C_i \rightarrow min$$

где Ci - затраты на i-е средство защиты

2) - оценка и управление рисками

Риском в сфере ИБ *будем называть потенциальную возможность понести убытки из-за нарушения безопасности информационной системы (ИС).*

Принцип «разумной достаточности»

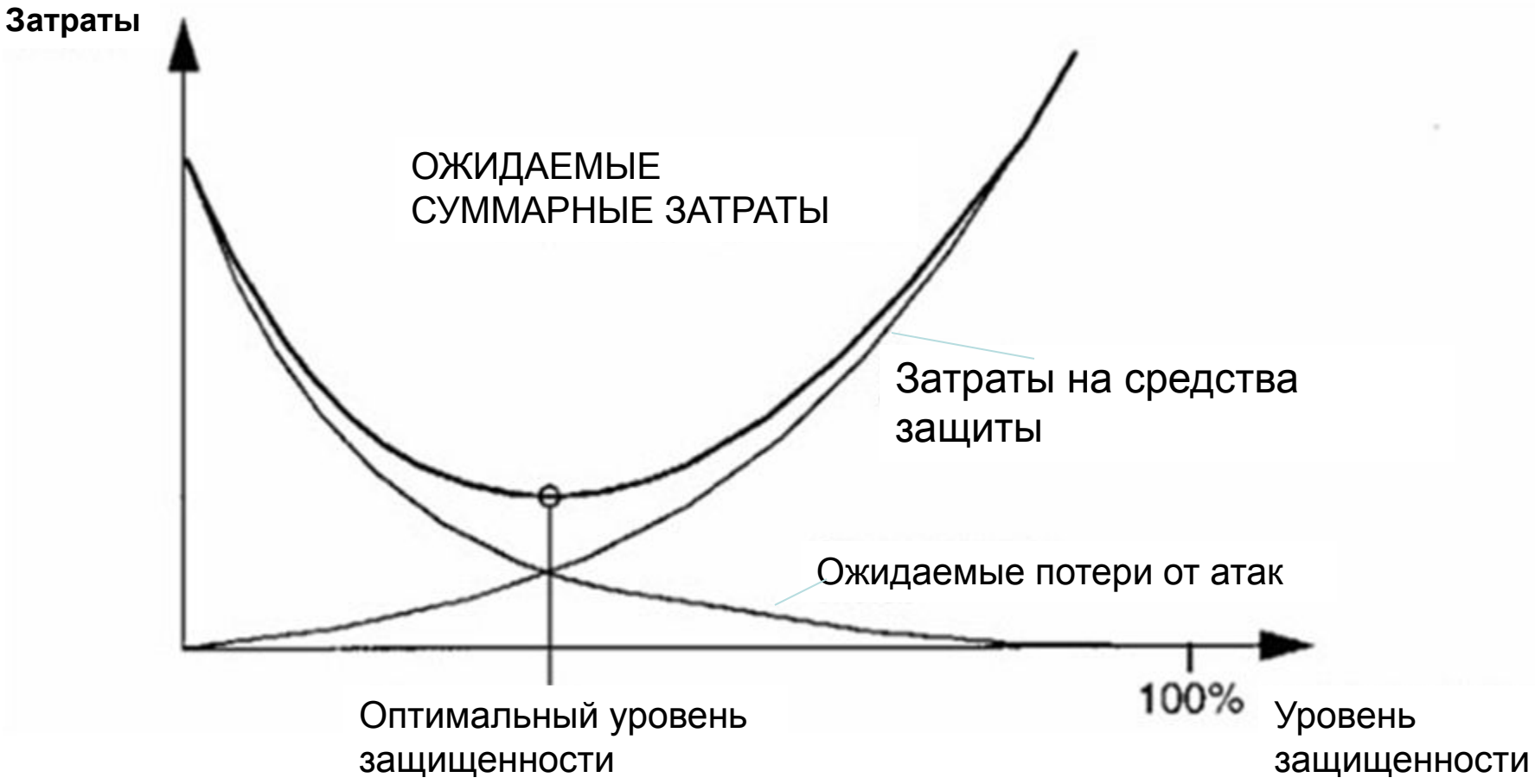
- абсолютно непреодолимой защиты создать невозможно;
- необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т.ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности;
- стоимость средств защиты не должна превышать стоимости защищаемой информации (или других ресурсов - аппаратных, программных);
- затраты нарушителя на несанкционированный доступ к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

Размер ущерба от реализации угрозы в отношении ресурса зависит от:

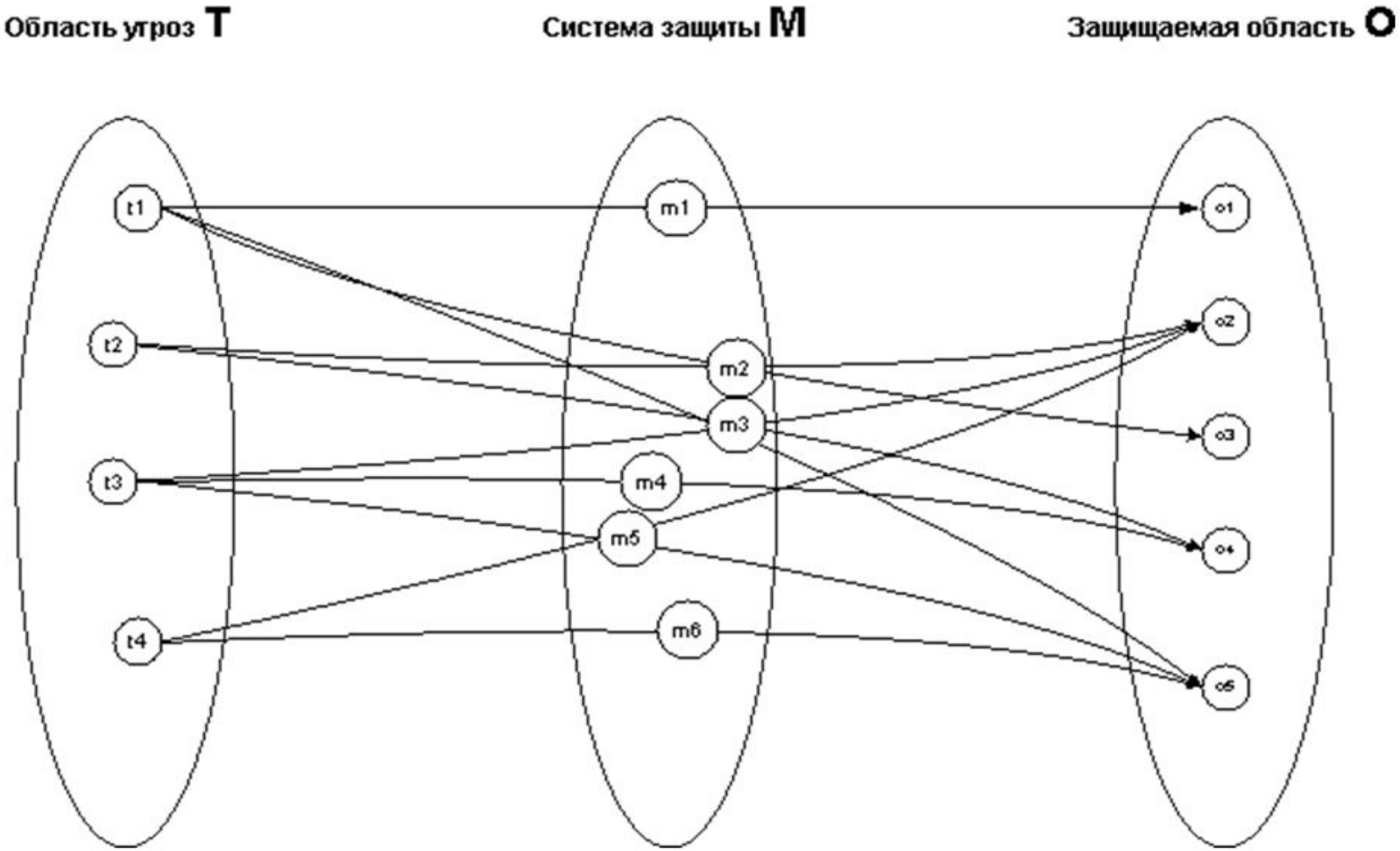
- стоимости ресурса, который подвергается риску.
- степени разрушительности воздействия на ресурс, выражаемой в виде коэффициента разрушительности. Как правило, указанный коэффициент лежит в диапазоне от 0 до 1.

Оценка= (Стоимость ресурса)*(Коэф. Разрушительности)

Стоимость риска=(Частота)*(Вероятность)*(Стоимость ресурса)*(Коэф. Разрушительности).


Затраты
ОЖИДАЕМЫЕ
СУММАРНЫЕ ЗАТРАТЫ
Затраты на средства
защиты
Ожидаемые потери от атак
100%
Оптимальный уровень
защищенности
Уровень
защищенности

III. Управление рисками в системе обеспечения информационной безопасности



- Модель системы защиты с полным перекрытием

модель защищенной системы –

система обеспечения безопасности Клементса

S={O,T,M,V,B}, *где*

O *- набор защищаемых объектов;*

T *- набор угроз;*

M *- набор средств обеспечения безопасности;*

V *- набор уязвимых мест = отображение* ***TxO*** *на набор упорядоченных пар* $Vi=(t_i, o_j)$, *представляющих собой пути проникновения в систему;*

B *- набор барьеров = отображение* ***VxM*** *или* ***TxOxM*** *на набор упорядоченных троек* $bi=(t_i, o_j, m_k)$ *представляющих собой точки, в которых требуется осуществлять защиту в системе.*

- Таким образом, система с полным перекрытием - это система, в которой имеются средства защиты на каждый возможный путь проникновения.

В системах с неполным перекрытием:

Надежность барьера характеризуется величиной остаточного риска :

$$Risk_l = P_{k^*} L_k (1-R_k)$$

R_l – степень сопротивляемости механизма защиты

P_k -Вероятность появления угрозы

L_k - величина ущерба

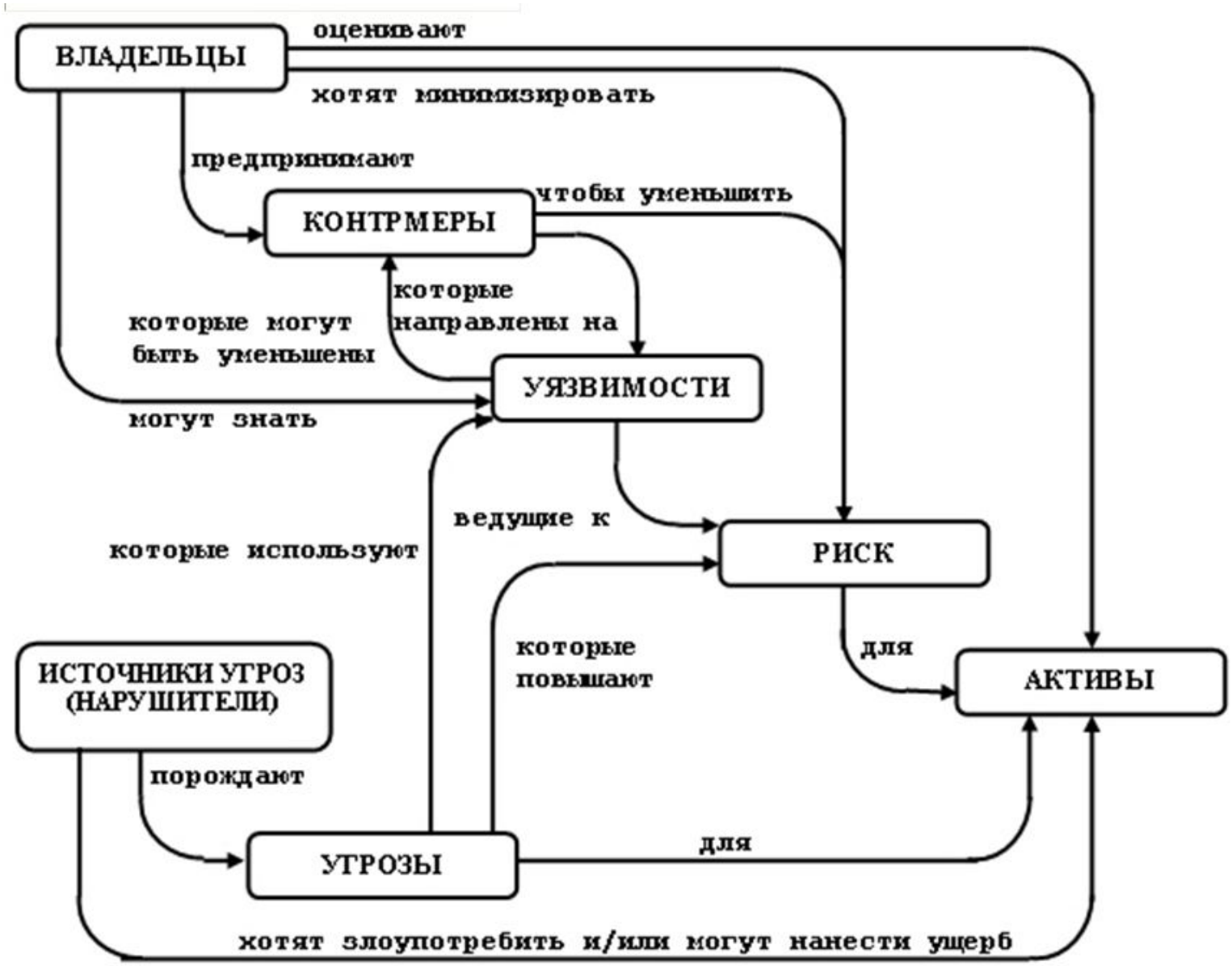
Примерная величина защищенности $S = 1 / Risk_0$

IV. ТРЕБОВАНИЯ К АРХИТЕКТУРЕ ИС С ТОЧКИ ЗРЕНИЯ ИБ:

- Проектирование ИС на принципах открытых систем
- Непрерывность защиты в пространстве и времени
- Усиление самого слабого звена, минимизация привилегий доступа
- Эшелонирование обороны. Разнообразие защитных средств,
- Простота и управляемость ИС и системой ее безопасности

V. ИНТЕГРАЛЬНАЯ БЕЗОПАСНОСТЬ ИС

ИИБ − это состояние условий функционирования человека, объектов, технических средств и систем, при котором они надежно защищены от всех возможных видов угроз в ходе непрерывной совокупности различных информационных процессов.



- Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002

В стандарте выделены 11 классов функциональных требований:

- аудит безопасности;
- связь (передача данных);
- криптографическая поддержка (криптографическая защита);
- защита данных пользователя;
- идентификация и аутентификация;
- управление безопасностью;
- приватность (конфиденциальность);
- защита функций безопасности объекта;
- использование ресурсов;
- доступ к объекту оценки;
- доверенный маршрут/канал.